Data Foundry, Inc.
1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
http://www.datafoundry.com

October 2, 2008

Via email: behavioralmarketingprinciples@ftc.gov

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles

Comments of Data Foundry, Inc.

Dear Secretary Clark:

Data Foundry has long been an advocate of Internet privacy and welcomes this opportunity to comment on the Federal Trade Commission's proposed principles for self-regulation of behavioral advertising. Data Foundry sees behavioral advertising as one issue, among many, that demonstrates the need for clear and coherent privacy protections for America's Internet users. The Commission should be commended for its foresight and initiative in addressing this important and difficult topic.

I. Introduction

Internet users should always have the right to know how and when their personal information is collected and must be able to choose whether to disclose and – just as important – control how any information they do disclose is subsequently used. Without clear and complete notice, users cannot make informed and meaningful decisions about what personal information to disclose and on what terms. Requiring affirmative express consent before personal

information is gathered and ensuring users know how information will be used empowers Internet users and provides important safeguards against abuse.

The FTC's call for comments has generated a vibrant discussion covering a wide range of issues, but Data Foundry sees a glaring omission in the dialogue. We will use these comments to address the matter that has so far been ignored. To date, the discussion of behavioral advertising has been limited to practices carried out on the "World Wide Web." Practices on the Internet[1] at large and – more important – by Internet Access Providers ("IAPs") have received little if any specific attention. These two distinctions are important because behavioral advertising systems have recently begun to emerge on the networks of various IAPs. These new systems use Deep Packet Inspection (DPI) to intercept and surveil all user traffic, regardless of the application protocol. Then – for the subset that is "Web" – the systems conduct a behavioral analysis and inject new content (i.e. targeted advertisements). This interception occurs "in the middle" of the Internet communication; it is unlike what happens when a user visits a web portal and, as part of user-to-portal interaction, intends to convey to or receive information from that portal. This much different kind of behavioral advertising is exceptionally invasive and poses a very serious threat to users' legal privacy rights of confidentiality and privilege. Data Foundry submits these comments to address the unacceptable consequences that network-based behavioral advertising and DPI will have for user privacy. We request the FTC to take discrete steps to ensure accountability and to protect consumers from this form of behavioral advertising.

[1] As the FTC undoubtedly knows, the "Web" is only a part of the "Internet." What most people consider to be the Web is merely one of several TCP/IP Application Layer Protocols, e.g., HTTP. There are many other application layer protocols as well, including NNTP, SIP, SSI, DNS, FTP, Gopher, NFS, NTP, DHCP, SMPP, SMTP, SNMP and Telnet.

II. Balancing the Role of Online Advertising with User Privacy

The vital function that advertising plays in promoting free content has been well recognized. Online advertising subsidizes much of the web by providing a source of revenue for small content producers. Through advertisement serving programs, like Google's Adsense, many independent web content creators are able to fully devote themselves to their unique endeavors. Many in the blogosphere have turned their websites into quite lucrative ventures, solely through the inclusion of web advertising systems that often include some form of contextual or behavioral targeting. In fact, the benefits of online marketing have become so well established and understood that a type of web-etiquette has developed alongside these systems, in which users will click on ads presented by websites they enjoy as a way to "tip" the authors. This symbiotic relationship between advertising and independent content has supported many of the most popular and innovative sites on the web.

As the FTC has recognized, balancing the content-driving qualities of online advertising against the privacy rights of individual Internet users is of paramount concern and necessary to ensure a vibrant and secure Internet.[2] Not all behavioral advertising platforms produce the same content-driving qualities: some pose much greater threats to user privacy than others. For example, while web-based advertising systems subsidize content creators and have a positive effect on the variety and availability of web content, network-based systems do not. These systems are placed "in the middle" of the communication and pass their ad revenue directly to the IAPs and, thus, entirely circumvent the content producers. They deprive individual web creators of income that the user often intends the creator to receive. Network-based systems will

[2] *See* Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles, http://www.ftc.gov/os/2007/12/P859900stmt.pdf ("In the online environment, innovation in consumer services and products – photo-sharing, blogging, the creation of virtual communities, and robust search, to name but a few – has significantly enhanced consumers' use of the Web. The FTC's privacy program seeks to balance support for such innovation with the need to protect harms to consumers' privacy.") (last visited September 30, 2008).

ultimately reduce the amount, quality and diversity of subsidized content that appears on the web. This type of behavioral advertising presents a very serious threat to Internet privacy that will have certain and severe consequences upon users' legal privacy rights of confidentiality and privilege.

III. The Need for Accountability and Enforcement

The FTC has wisely eschewed heavy-handed administrative agency level regulation in favor of a market-based framework. This current self-regulatory regime, however, lacks any meaningful methods of enforcing the FTC's Fair Information Practice Principles. This has encouraged behavioral advertising systems vendors and IAPs to push the privacy envelope. Internet users will suffer when online privacy rights are disregarded in favor of more and more invasive forms of behavioral advertising, but they have no real recourse. Unless IAPs can be held accountable to their customers, privacy rights will be cast aside in an online advertising race to the bottom, which is exactly what is now happening with DPI-facilitated behavioral targeting. But as we show below, this accountability need not come from active agency oversight. Instead, a declaration of public policy – that can then be enforced and litigated through standard consumer law (just like all other "unregulated" contracts) is far preferable.

IV. Network-Based Behavioral Advertising Draws Ire

Over the past year, network-based behavioral adverting vendors have partnered with a number of IAPs to implement DPI-facilitated targeted advertising systems on various IAPs' networks.[3] The advertising vendors, such as NebuAd, Phorm and Front Porch, have contracted with IAPs for the right to attach DPI appliances at their facilities and to split advertising revenue on a per user basis. This practice has received a great deal of public condemnation in recent

[3] The first of these business arrangements occurred in the United Kingdom over the summer of 2007, between IAP British Telecom (BT) and advertising vendor Phorm. This relationship was not disclosed until February, 2008. Since that time a number of similar business relationship have come to light in the United States.

months, following Charter Communications' announcement that NebuAd would be conducting DPI on its network and behaviorally targeting Charter's users. Based on the concern that these systems violate user privacy rights, a congressional inquiry into DPI-facilitated behavioral advertising practices was launched over the summer.[4]

In contrast to web-based systems, network-based behavioral advertising has generated widespread public criticism due to the way that it intercepts traffic between communicating parties. With web-based systems, *one of the intended communicants* is performing the behavioral targeting. For the most part users understand they are providing the other party (i.e. the website) with personal information in the same way that they would in any other real world interaction. The degree of privacy present in these communications is determined by the mutually-understood intentions of the parties. If users do not wish to be subject to this behavioral advertising, they are free to exercise consumer choice and abstain from traveling to such sites.

But with network-based advertising, an unintended third party injects itself into the communication. Regardless of the degree of privacy intended and understood by the original parties, communications are subject to inspection and are then used for behavioral targeting. Users that want to protect their communications have no means to avoid or limit the practice short of terminating their Internet access service and doing without.

Due to extensive negative publicity and the ongoing congressional inquiry, NebuAd recently announced its intention to temporarily abandon its DPI-facilitated advertising product in

[4] *See* U.S. Senate Committee on Commerce, Science & Transportation Website, Privacy Implications of Online Advertising, http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=e46b0d9f-562e-41a6-b460-a714bf370171 (last visited September 30, 2008) ("In this hearing, the Committee will consider the current state of the online advertising industry and that market's impact on users' privacy. Witnesses are expected to focus on the key factors driving online behavioral advertising, the methods of online behavioral advertising employed by industry, and the protections the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) should adopt to protect consumers from unwanted or unnecessary invasions of their privacy.").

favor of more traditional methods of behavioral advertising (i.e. web-based adverting).[5] Similarly, several of the IAPs that had partnered with companies like NebuAd also announced their own plans to end their use of the DPI-facilitated behavioral advertising systems on their networks.[6] However, the IAPs insisted that the cessation is temporary and they retained the right to once again conduct network-based behavioral advertising on their networks in the future.[7] IAPs fully intend to turn their DPI-facilitated ad systems back on, once the issue recedes from the public spotlight.

V. Deep Packet Inspection

To appreciate the privacy threat posed by network-based behavioral advertising, one must first understand how DPI operates to intercept the content of users' communications. DPI is an incredibly powerful tool that was originally designed to function as a type of network firewall that could identify and filter out harmful IP packets based on their contents.[8] The technology has proven to be so adept at inspecting network traffic and creating a comprehensive picture of the contents that it has begun to be put to a number of other uses, including behavioral advertising. At its heart, though, DPI is a tool for monitoring the content of users' Internet traffic in real time.

---

5 *See* Ellen Nakashima, NebuAd Halts Plans for Web Tracking, WashingtonPost.com, September 4, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html?hpid=sec-tech (last visited September 30, 2008).

6 *See e.g.* Saul Hansell, Charter Suspends Plan to Sell Customer Data to Advertisers, NYTimes.com, June 24, 2008, http://bits.blogs.nytimes.com/2008/06/24/charter-suspends-plan-to-sell-customer-data-to-advertisers/ (last visited September 30, 2008); Wendy Davis, Under Pressure: Charter Delays Info Sharing With NebuAd, MediaPost.com, June 17, 2008, http://www.mediapost.com/publications/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=84797 (last visited September 30, 2008).

7 *See e.g.* Karl Bode, Another ISP Suspends NebuAd Trials, DSLReports.com, June 30, 2008, http://www.dslreports.com/shownews/Another-ISP-Suspends-NebuAD-Trials-95674 (last visited September 30, 2008) (CenturyTel emails informed users that, "CenturyTel is not currently using online behavioral advertising tools in any of its markets, and we are delaying our plans to move forward with the deployment of online behavioral advertising services - either through NebuAd or any other vendor - at this time. CenturyTel is delaying its implementation plans so that Congress can spend additional time addressing the privacy issues and policies associated with online behavioral advertising.") (emphasis added).

The uses that can then be put to the knowledge gleaned from DPI are almost limitless. Admittedly, some might be beneficial, but many others portend great harm.

DPI is often and easily analogized to the opening and inspection of one's postal mail. IP packets, which carry Internet communications, were designed to operate much like letters and envelopes carried by a postal service. Packet headers contain basic addressing information, including the IP addresses of the sender and recipient and simple handling instructions, just as envelopes in the mail do. As an IP packet travels the Internet en route to its intended recipient, all that the handling IAPs must examine is the addressing data in the header (i.e. the envelope information). This is often referred to as shallow packet inspection. Simple delivery has never required the IAPs to look beyond the header information. Packet bodies, on the other hand, contain the communication's contents, much like an actual letter within an envelope. DPI delves past the header to read the body and the contents of the communication, which is akin to the post office opening and reading envelopes that go through the mail.

VI. Monitoring Private Communications

To conduct network-based behavioral advertising, DPI reads the contents of the Internet traffic crossing the network to generate very specific profiles of each user and to insert acutely tailored ads. Users are intrusively surveiled while they surf the web, send and receive emails, communicate by chat or VoIP, download or upload files, and attach devices to the Internet. It is the functional – albeit perhaps not the legal – equivalent of a combination wiretap, trap and trace and pen register installed by the IAP for its own private use.[9] As former NebuAd CEO Bob Dykes explained, "We understand what pages you went to. We understand all the search terms you entered. … We actually see not only that you went to all these sites, we know what you did

[9] Data Foundry notes that in this instance the information is not routinely requested by or even given to law enforcement. The propriety of DPI surveillance while cooperating with governmental authorities is not what we are addressing here.

on the sites."[10] With these advertising systems, everything that a user does and looks at on the Internet is monitored for advertising purposes, which threatens to fundamentally change how the law regards the private and confidential nature of those communications.

Using the Internet often involves deeply personal matters that Americans expect to remain private. Users communicate in confidence with their spouses, medical professionals, attorneys, clergymen, and explore interests and ideas that they may prefer to keep from others. To reassure users, DPI-facilitated behavioral advertising vendors have claimed that they proactively anonymize user information and filter out communications that they deem to be sensitive.[11] This response, however, demonstrates exactly why network-based behavioral advertising is such a serious threat to privacy. As incredibly accurate personal information is culled and inspected by DPI, users are left hoping that businesses – which are insulated from accountability and have material interests fundamentally opposed to the users' privacy – will act in good faith to protect and purge their private data. Given that this information is in fact monitored and inspected, and not redacted until sometime later, it is understandable why users would be concerned with the privacy of their communications and information.

---

[10] *See* Vator.tv website, NebuAd page embedded video at 2:27 and 3:25, http://www.vator.tv/pitch/show/transforming-online-ad-industry?play=false (last visited September 30, 2008).

[11] *See* Vator.tv website, NebuAd page embedded video at 0:14 and 0:51, http://www.vator.tv/pitch/show/transforming-online-ad-industry?document=nebuad-at-new-york-city-ao (last visited September 30, 2008) ("We are able to combine people's search terms and the pages that they go to and what they do on those pages to really build deep behavioral profiles. We do this in conjunction with service providers. We operate with them in a real time mode. …So we provide very deep profiles, completely anonymous, however. [We] operate with complete privacy."

VII. IAP Contracts Force Users to Consent to Inspection and Forfeit Their Privacy

a. The Contractual Waiver of User Privacy Rights

Until Charter announced its partnership with NebuAd, users had generally never received meaningful notice of network-based behavioral advertising and were not offered the opportunity to opt-out of the practice.[12] The behavioral advertising vendors uniformly declined to disclose their business relationships and asserted that the burden to inform users fell to the IAPs, rather than themselves.[13] The IAPs, for their part, have also generally failed to identify any parties that were allowed access to their network, which left many Internet users totally unaware that their online communications were being monitored.[14] When this issue was brought before the congressional inquiry, the IAPs pointed to the fine print of their non-negotiable subscriber contracts as the authorization for network inspection and behavioral advertising.[15]

The IAPs were correct: their subscriber agreements do in fact authorize DPI and behavioral advertising and many other potentially objectionable network practices that are not directly relevant to the inquiry at hand.[16] These broad contracts are chock-full of legalese and are

---

[12] *See* Karl Bode, Embarq, WOW Bury Snooping in Terms of Service, DSLReports.com, http://www.dslreports.com/shownews/Embarq-WOW-Bury-Snooping-In-Terms-Of-Service-93375 (last visited September 30, 2008).

[13] *See* Declan McCullagh, Web Monitoring for Ads? It May Be Illegal, CNet.com, http://news.cnet.com/8301-13578_3-9947499-38.html (last visited September 30, 2008) ("NebuAd refused to disclose what advertising networks--such as DoubleClick or Microsoft's Aquantive--it uses, or what broadband providers it counts as customers. So did Phorm and Front Porch (which said it could not arrange an interview). When asked why it won't disclose that information, NebuAd told us in e-mail: 'We would like to respect the trust and relationship that already exists between an ISP and their end customer. We want to stress that we do not publicly discuss our ISP partner relationships because of the direct relationship that already exists between an ISP and their customers. Our belief is that our ISP partners have a direct, trusted relationship with their customers; and communication, public or otherwise, should be directly from our ISP partner to their end customer.'").

[14] *See e.g.* AT&T Privacy Policy for AT&T Yahoo! *infra* note 16, http://helpme.att.net/article.php?item=8620 (last visited September 30, 2008).

[15] *See* Embarq response to letter from congressmen Joe Barton, Edward Markey and John Dingell, BroadcastingCable.com, http://www.broadcastingcable.com/contents/pdf/EmbarqResponse.pdf (last visited September 30, 2008).

[16] *See e.g.* AT&T Privacy Policy for AT&T Yahoo! and Video Services, For All Applications, All Operating Systems, and All Domains, http://helpme.att.net/article.php?item=8620 (last visited September 30, 2008) ("AT&T uses Usage Information to personalize your Services, to recommend content, and to select advertisements or other

sometimes unclear, but a close reading reveals that they are in fact placing users on notice that their communications can and often will be inspected for any reason.[17] The user functionally waives any and all privacy expectations against the IAP. AT&T's subscriber agreement goes so far as to claim ownership over user communications, which are deemed to be the business records of AT&T.[18] The IAPs' subscriber contracts require users to waive privacy by consenting to the monitoring of their online activities. ***This is a mandatory condition of receiving service.***

b. The Destruction of All Online Privacy Rights

The IAPs typically make promises and commitments regarding the use they will make of the private information they capture. While that is laudable, it does not serve to preserve or "unwaive" privacy.[19] Under the law, once confidentiality has been waived as to one party or destroyed through inspection, it is waived as to all.[20] While IAP privacy policies and the behavioral advertising vendors may make certain promises to protect or respect the privacy of the users, these reassurances are wholly ineffective because confidentiality has already been destroyed by user consent to inspection. Under what has been termed the Third Party Doctrine, one cannot maintain a reasonable expectation of privacy in any information that is knowingly

---

promotions for you based upon your interests. … We may disclose Aggregated Information to third parties including advertisers, content providers, market research companies and other organizations.").

[17] A recent report analyzed the readability of various IAP privacy policies and determined that almost all required at least a college level education to understand the policies. A number were scored at post-graduate levels of readability. *See* Erik Sherman, Privacy Policies are Great – PhDs, BNet.com, http://industry.bnet.com/technology/1000391/privacy-policies-are-great-for-phds/ (last visited September 30, 2008).

[18] *See* AT&T Privacy Policy for AT&T Yahoo! *supra* note 16, http://helpme.att.net/article.php?item=8620 (last visited September 30, 2008) ("While your Account Information may be personal to you, these records constitute business records that are owned by AT&T. As such, AT&T may disclose such records to protect its legitimate business interests, safeguard others, or respond to legal process.").

[19] *See* Jennifer A. Hardgrove, *Scope of Waiver of Attorney-Client Privilege: Articulating a Standard That Will Afford Guidance to Courts*, 1998 U. Ill. L. Rev. 643, 653 (1998) ("Voluntary disclosure of a privileged communication constitutes a waiver in nearly all situations, even where the disclosure was nontruthful or misstated, where the disclosed information could have been obtained elsewhere, and where the third party receiving the disclosed information agreed not to further disclose it.") (Emphasis added).

[20] Because confidentiality requires that a communication stay entirely out of the purview of *any* unintended parties, once the confidence has been vitiated through disclosure, it cannot be reestablished. The presence of the unintended party will always frustrate confidentiality as to all relationships. In this respect, confidentiality is much like Humpty Dumpty, once it has been broken, it cannot be put back together again.

disclosed to a third party. Because users are required to consent to DPI and the monitoring of their online communications, they have knowingly disclosed this private information to a third party. The result is that any expectation of privacy the user may have is unreasonable as a matter of law.

This combination of inspection and waiver now threatens to profoundly change the way online privacy rights are determined. Heretofore the courts have assumed that contents are not generally inspected and Internet communications have traditionally been held to the same privacy and privilege standard as private telephone and mail communications. The information can be obtainable only by warrant[21] or a subpoena directed at one of the communicants. With the introduction of DPI to perform behavioral advertising, user communications are no longer carried without inspection. Confidentiality is destroyed through third party access.[22] Because confidentiality is an essential element of common law and statutory privileges, an inspected Internet is incapable of carrying privileged communications.[23] Those who wish to maintain privileged relationships can no longer communicate in confidence over an Internet that is monitored by their IAPs. These communications will be treated as all other non-confidential

---

[21] See *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) ("In a sense, e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission. The sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police."); *United States v. Charbonneau*, 979 F.Supp. 1177, 1184 (D. Ohio 1997) ("E-Mail is almost equivalent to sending a letter via the mails.").

[22] *See United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) ("The policy clearly stated that FBIS would "audit, inspect, and/or monitor" employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate." J.A. 127. This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private.").

[23] The leading privilege test was established in *United States v. United Shoe Machinery Corp.* 89 F. Supp. 357, 358-59 (D. Mass. 1950). The *United Shoe* test provides that a privilege (in this instance between an attorney and a client) applies if:

> (1) the asserted holder of the privilege is or sought to become a client; (2) the person to whom the communication was made (a) is the member of the bar of court, on his subordinate and (b) in connection with this communication is acting as a lawyer; (3) the communication relates to a fact of which the attorney was informed (a) by his client (b) without the presence of strangers (c) for the purpose of securing primarily either (i) an opinion of law or (ii) legal services or (iii) assistance in some legal preceding, and not (d) for the propose of committing a crime or tort; and (4) the privilege has been (a) claimed and (b) not waived by the client. (emphasis added).

communications and will be freely accessible to outside parties with a subpoena to the IAP based on a mere showing that production *may* lead to the discovery of relevant evidence.[24] The communication will be disclosed before the privilege holder ever gets notice or a chance to assert the privilege. Important confidential and privileged communications would be available to anyone under the very lax standard of mere relevance. Any and all privileges will have been waived by simply accessing the inspected network.

It is not just the confidentiality of communications between private individuals that are threatened by DPI and network-based behavioral advertising. The Internet has been incorporated into virtually every American industry as a means of efficiently carrying out transactions and communications. Businesses use the Internet to communicate externally with consumers and other companies, as well as internally amongst employees and facilities. A huge portion of these online communications contain proprietary information and trade secrets that are intended to remain confidential, often being subject to non-disclosure agreements. But with an IAP inspected Internet, even business trade secrets and other confidential business information loses all protection. Ecommerce may grind to a halt because sensitive information will have to be communicated "the old fashioned way." That could very well put the nail in our country's economic coffin.

VIII. Declaration of Public Policy Against Abusive Subscriber Contracts

Under the current self-regulatory framework, those that would violate the privacy rights of America's Internet users are subject to little accountability. IAPs and advertising systems

[24] *See* Fed. Rules Civ. Proc. R. 26(b)(1) ("Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.") (Emphasis added).

vendors are free to wiretap their users communications and peer into their most private online activities with no fear of repercussion. Users cannot adequately protect their privacy rights and guard themselves against potentially abusive network practices and subscriber contracts.

While DPI and network-based behavioral advertising need not be prohibited, they should only be permitted once users have expressly and knowingly opted-in to the practices. Requiring this consent as a mandatory condition of service is not voluntary and is fundamentally opposed to the FTC's proposed principles of affirmative express consent and consumer control. Ensuring voluntary and informed user consent to potentially harmful subscriber contracts and network practices falls in line with the intent of the proposed principles and the expectations of Internet users.

To ensure that the new privacy principles, as well as the Fair Information Practice Principles, are uniformly observed throughout the industry, the FTC has a responsibility to provide users with a means to protect themselves against mistreatment. While intrusive regulation would likely stifle innovation and lead to burdensome administrative oversight, there is a solution that can protect user privacy and is consistent with the notion of deregulation. Data Foundry requests that the FTC formally recognize a public policy against abusive Internet access contracts that require consumers to waive their privacy rights as a condition of service and provide inadequate disclosure of network practices and their subsequent effects upon user privacy.

Public policies are privately enforceable in state and federal courts of law without any need for further administrative or regulatory action. Individual citizens that are injured by these exploitative subscriber agreements and behavioral advertising practices would have the right to bring claims against their IAPs under traditional principles of contract law that prohibit

violations of established public policies. This stated policy would merely hold IAPs and advertising vendors accountable to their customers through judicial remedies, in the same manner as all other deregulated contract relationships. The policy would protect the privacy of online communications from an especially insidious form of invasion and provide a much-needed safeguard against abuse, without the need for burdensome regulation.

IX. Conclusion

Data Foundry is grateful to the FTC for the opportunity to address these important and involved matters. The privacy issues inherent in behavioral advertising present difficult challenges to ensuring an innovative and safe Internet. We hope that the FTC will recognize the particularly invasive nature of DPI-facilitated behavioral advertising and the harmful effects of the subscriber agreements that require users consent to inspection and waive their privacy rights as conditions of service. By declaring a public policy against such contracts (rather than trying to devise *ex post* and *ex ante* rules and procedures and an administrative enforcement process), the FTC would be treating Internet access like all other "unregulated" activities. It would be a simple matter of contract and consumer law, handled at the state level. But it would provide Internet users with the necessary means to protect their privacy. At the same time, it would ensure that "the Internet" is not burdened by intrusive administrative regulation.

Respectfully Submitted,

/s/
Ron Yokubaitis
Chairman and CEO, Data Foundry, Inc.

Data Foundry, Inc.
1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
http://www.datafoundry.com

October 2, 2008

Via email: behavioralmarketingprinciples@ftc.gov

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles

Comments of Data Foundry, Inc.

Dear Secretary Clark:

Data Foundry has long been an advocate of Internet privacy and welcomes this opportunity to comment on the Federal Trade Commission's proposed principles for self-regulation of behavioral advertising. Data Foundry sees behavioral advertising as one issue, among many, that demonstrates the need for clear and coherent privacy protections for America's Internet users. The Commission should be commended for its foresight and initiative in addressing this important and difficult topic.

I. Introduction

Internet users should always have the right to know how and when their personal information is collected and must be able to choose whether to disclose and – just as important – control how any information they do disclose is subsequently used. Without clear and complete notice, users cannot make informed and meaningful decisions about what personal information to disclose and on what terms. Requiring affirmative express consent before personal

information is gathered and ensuring users know how information will be used empowers Internet users and provides important safeguards against abuse.

The FTC's call for comments has generated a vibrant discussion covering a wide range of issues, but Data Foundry sees a glaring omission in the dialogue. We will use these comments to address the matter that has so far been ignored. To date, the discussion of behavioral advertising has been limited to practices carried out on the "World Wide Web." Practices on the Internet[1] at large and – more important – by Internet Access Providers ("IAPs") have received little if any specific attention. These two distinctions are important because behavioral advertising systems have recently begun to emerge on the networks of various IAPs. These new systems use Deep Packet Inspection (DPI) to intercept and surveil all user traffic, regardless of the application protocol. Then – for the subset that is "Web" – the systems conduct a behavioral analysis and inject new content (i.e. targeted advertisements). This interception occurs "in the middle" of the Internet communication; it is unlike what happens when a user visits a web portal and, as part of user-to-portal interaction, intends to convey to or receive information from that portal. This much different kind of behavioral advertising is exceptionally invasive and poses a very serious threat to users' legal privacy rights of confidentiality and privilege. Data Foundry submits these comments to address the unacceptable consequences that network-based behavioral advertising and DPI will have for user privacy. We request the FTC to take discrete steps to ensure accountability and to protect consumers from this form of behavioral advertising.

[1] As the FTC undoubtedly knows, the "Web" is only a part of the "Internet." What most people consider to be the Web is merely one of several TCP/IP Application Layer Protocols, e.g., HTTP. There are many other application layer protocols as well, including NNTP, SIP, SSI, DNS, FTP, Gopher, NFS, NTP, DHCP, SMPP, SMTP, SNMP and Telnet.

II. Balancing the Role of Online Advertising with User Privacy

The vital function that advertising plays in promoting free content has been well recognized. Online advertising subsidizes much of the web by providing a source of revenue for small content producers. Through advertisement serving programs, like Google's Adsense, many independent web content creators are able to fully devote themselves to their unique endeavors. Many in the blogosphere have turned their websites into quite lucrative ventures, solely through the inclusion of web advertising systems that often include some form of contextual or behavioral targeting. In fact, the benefits of online marketing have become so well established and understood that a type of web-etiquette has developed alongside these systems, in which users will click on ads presented by websites they enjoy as a way to "tip" the authors. This symbiotic relationship between advertising and independent content has supported many of the most popular and innovative sites on the web.

As the FTC has recognized, balancing the content-driving qualities of online advertising against the privacy rights of individual Internet users is of paramount concern and necessary to ensure a vibrant and secure Internet.[2] Not all behavioral advertising platforms produce the same content-driving qualities: some pose much greater threats to user privacy than others. For example, while web-based advertising systems subsidize content creators and have a positive effect on the variety and availability of web content, network-based systems do not. These systems are placed "in the middle" of the communication and pass their ad revenue directly to the IAPs and, thus, entirely circumvent the content producers. They deprive individual web creators of income that the user often intends the creator to receive. Network-based systems will

[2] *See* Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles, http://www.ftc.gov/os/2007/12/P859900stmt.pdf ("In the online environment, innovation in consumer services and products – photo-sharing, blogging, the creation of virtual communities, and robust search, to name but a few – has significantly enhanced consumers' use of the Web. The FTC's privacy program seeks to balance support for such innovation with the need to protect harms to consumers' privacy.") (last visited September 30, 2008).

ultimately reduce the amount, quality and diversity of subsidized content that appears on the web. This type of behavioral advertising presents a very serious threat to Internet privacy that will have certain and severe consequences upon users' legal privacy rights of confidentiality and privilege.

III. The Need for Accountability and Enforcement

The FTC has wisely eschewed heavy-handed administrative agency level regulation in favor of a market-based framework. This current self-regulatory regime, however, lacks any meaningful methods of enforcing the FTC's Fair Information Practice Principles. This has encouraged behavioral advertising systems vendors and IAPs to push the privacy envelope. Internet users will suffer when online privacy rights are disregarded in favor of more and more invasive forms of behavioral advertising, but they have no real recourse. Unless IAPs can be held accountable to their customers, privacy rights will be cast aside in an online advertising race to the bottom, which is exactly what is now happening with DPI-facilitated behavioral targeting. But as we show below, this accountability need not come from active agency oversight. Instead, a declaration of public policy – that can then be enforced and litigated through standard consumer law (just like all other "unregulated" contracts) is far preferable.

IV. Network-Based Behavioral Advertising Draws Ire

Over the past year, network-based behavioral adverting vendors have partnered with a number of IAPs to implement DPI-facilitated targeted advertising systems on various IAPs' networks.[3] The advertising vendors, such as NebuAd, Phorm and Front Porch, have contracted with IAPs for the right to attach DPI appliances at their facilities and to split advertising revenue on a per user basis. This practice has received a great deal of public condemnation in recent

[3] The first of these business arrangements occurred in the United Kingdom over the summer of 2007, between IAP British Telecom (BT) and advertising vendor Phorm. This relationship was not disclosed until February, 2008. Since that time a number of similar business relationship have come to light in the United States.

months, following Charter Communications' announcement that NebuAd would be conducting DPI on its network and behaviorally targeting Charter's users. Based on the concern that these systems violate user privacy rights, a congressional inquiry into DPI-facilitated behavioral advertising practices was launched over the summer.[4]

In contrast to web-based systems, network-based behavioral advertising has generated widespread public criticism due to the way that it intercepts traffic between communicating parties. With web-based systems, *one of the intended communicants* is performing the behavioral targeting. For the most part users understand they are providing the other party (i.e. the website) with personal information in the same way that they would in any other real world interaction. The degree of privacy present in these communications is determined by the mutually-understood intentions of the parties. If users do not wish to be subject to this behavioral advertising, they are free to exercise consumer choice and abstain from traveling to such sites.

But with network-based advertising, an unintended third party injects itself into the communication. Regardless of the degree of privacy intended and understood by the original parties, communications are subject to inspection and are then used for behavioral targeting. Users that want to protect their communications have no means to avoid or limit the practice short of terminating their Internet access service and doing without.

Due to extensive negative publicity and the ongoing congressional inquiry, NebuAd recently announced its intention to temporarily abandon its DPI-facilitated advertising product in

[4] *See* U.S. Senate Committee on Commerce, Science & Transportation Website, Privacy Implications of Online Advertising, http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=e46b0d9f-562e-41a6-b460-a714bf370171 (last visited September 30, 2008) ("In this hearing, the Committee will consider the current state of the online advertising industry and that market's impact on users' privacy. Witnesses are expected to focus on the key factors driving online behavioral advertising, the methods of online behavioral advertising employed by industry, and the protections the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) should adopt to protect consumers from unwanted or unnecessary invasions of their privacy.").

favor of more traditional methods of behavioral advertising (i.e. web-based adverting).[5] Similarly, several of the IAPs that had partnered with companies like NebuAd also announced their own plans to end their use of the DPI-facilitated behavioral advertising systems on their networks.[6] However, the IAPs insisted that the cessation is temporary and they retained the right to once again conduct network-based behavioral advertising on their networks in the future.[7] IAPs fully intend to turn their DPI-facilitated ad systems back on, once the issue recedes from the public spotlight.

V. Deep Packet Inspection

To appreciate the privacy threat posed by network-based behavioral advertising, one must first understand how DPI operates to intercept the content of users' communications. DPI is an incredibly powerful tool that was originally designed to function as a type of network firewall that could identify and filter out harmful IP packets based on their contents.[8] The technology has proven to be so adept at inspecting network traffic and creating a comprehensive picture of the contents that it has begun to be put to a number of other uses, including behavioral advertising. At its heart, though, DPI is a tool for monitoring the content of users' Internet traffic in real time.

---

5 *See* Ellen Nakashima, NebuAd Halts Plans for Web Tracking, WashingtonPost.com, September 4, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html?hpid=sec-tech (last visited September 30, 2008).

6 *See e.g.* Saul Hansell, Charter Suspends Plan to Sell Customer Data to Advertisers, NYTimes.com, June 24, 2008, http://bits.blogs.nytimes.com/2008/06/24/charter-suspends-plan-to-sell-customer-data-to-advertisers/ (last visited September 30, 2008); Wendy Davis, Under Pressure: Charter Delays Info Sharing With NebuAd, MediaPost.com, June 17, 2008, http://www.mediapost.com/publications/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=84797 (last visited September 30, 2008).

7 *See e.g.* Karl Bode, Another ISP Suspends NebuAd Trials, DSLReports.com, June 30, 2008, http://www.dslreports.com/shownews/Another-ISP-Suspends-NebuAD-Trials-95674 (last visited September 30, 2008) (CenturyTel emails informed users that, "CenturyTel is not currently using online behavioral advertising tools in any of its markets, and we are delaying our plans to move forward with the deployment of online behavioral advertising services - either through NebuAd or any other vendor - at this time. CenturyTel is delaying its implementation plans so that Congress can spend additional time addressing the privacy issues and policies associated with online behavioral advertising.") (emphasis added).

The uses that can then be put to the knowledge gleaned from DPI are almost limitless. Admittedly, some might be beneficial, but many others portend great harm.

DPI is often and easily analogized to the opening and inspection of one's postal mail. IP packets, which carry Internet communications, were designed to operate much like letters and envelopes carried by a postal service. Packet headers contain basic addressing information, including the IP addresses of the sender and recipient and simple handling instructions, just as envelopes in the mail do. As an IP packet travels the Internet en route to its intended recipient, all that the handling IAPs must examine is the addressing data in the header (i.e. the envelope information). This is often referred to as shallow packet inspection. Simple delivery has never required the IAPs to look beyond the header information. Packet bodies, on the other hand, contain the communication's contents, much like an actual letter within an envelope. DPI delves past the header to read the body and the contents of the communication, which is akin to the post office opening and reading envelopes that go through the mail.

VI. Monitoring Private Communications

To conduct network-based behavioral advertising, DPI reads the contents of the Internet traffic crossing the network to generate very specific profiles of each user and to insert acutely tailored ads. Users are intrusively surveiled while they surf the web, send and receive emails, communicate by chat or VoIP, download or upload files, and attach devices to the Internet. It is the functional – albeit perhaps not the legal – equivalent of a combination wiretap, trap and trace and pen register installed by the IAP for its own private use.[9] As former NebuAd CEO Bob Dykes explained, "We understand what pages you went to. We understand all the search terms you entered. … We actually see not only that you went to all these sites, we know what you did

[9] Data Foundry notes that in this instance the information is not routinely requested by or even given to law enforcement. The propriety of DPI surveillance while cooperating with governmental authorities is not what we are addressing here.

on the sites."[10] With these advertising systems, everything that a user does and looks at on the Internet is monitored for advertising purposes, which threatens to fundamentally change how the law regards the private and confidential nature of those communications.

Using the Internet often involves deeply personal matters that Americans expect to remain private. Users communicate in confidence with their spouses, medical professionals, attorneys, clergymen, and explore interests and ideas that they may prefer to keep from others. To reassure users, DPI-facilitated behavioral advertising vendors have claimed that they proactively anonymize user information and filter out communications that they deem to be sensitive.[11] This response, however, demonstrates exactly why network-based behavioral advertising is such a serious threat to privacy. As incredibly accurate personal information is culled and inspected by DPI, users are left hoping that businesses – which are insulated from accountability and have material interests fundamentally opposed to the users' privacy – will act in good faith to protect and purge their private data. Given that this information is in fact monitored and inspected, and not redacted until sometime later, it is understandable why users would be concerned with the privacy of their communications and information.

---

[10] *See* Vator.tv website, NebuAd page embedded video at 2:27 and 3:25, http://www.vator.tv/pitch/show/transforming-online-ad-industry?play=false (last visited September 30, 2008).

[11] *See* Vator.tv website, NebuAd page embedded video at 0:14 and 0:51, http://www.vator.tv/pitch/show/transforming-online-ad-industry?document=nebuad-at-new-york-city-ao (last visited September 30, 2008) ("We are able to combine people's search terms and the pages that they go to and what they do on those pages to really build deep behavioral profiles. We do this in conjunction with service providers. We operate with them in a real time mode. …So we provide very deep profiles, completely anonymous, however. [We] operate with complete privacy."

VII. IAP Contracts Force Users to Consent to Inspection and Forfeit Their Privacy

a. The Contractual Waiver of User Privacy Rights

Until Charter announced its partnership with NebuAd, users had generally never received meaningful notice of network-based behavioral advertising and were not offered the opportunity to opt-out of the practice.[12] The behavioral advertising vendors uniformly declined to disclose their business relationships and asserted that the burden to inform users fell to the IAPs, rather than themselves.[13] The IAPs, for their part, have also generally failed to identify any parties that were allowed access to their network, which left many Internet users totally unaware that their online communications were being monitored.[14] When this issue was brought before the congressional inquiry, the IAPs pointed to the fine print of their non-negotiable subscriber contracts as the authorization for network inspection and behavioral advertising.[15]

The IAPs were correct: their subscriber agreements do in fact authorize DPI and behavioral advertising and many other potentially objectionable network practices that are not directly relevant to the inquiry at hand.[16] These broad contracts are chock-full of legalese and are

---

[12] *See* Karl Bode, Embarq, WOW Bury Snooping in Terms of Service, DSLReports.com, http://www.dslreports.com/shownews/Embarq-WOW-Bury-Snooping-In-Terms-Of-Service-93375 (last visited September 30, 2008).

[13] *See* Declan McCullagh, Web Monitoring for Ads? It May Be Illegal, CNet.com, http://news.cnet.com/8301-13578_3-9947499-38.html (last visited September 30, 2008) ("NebuAd refused to disclose what advertising networks--such as DoubleClick or Microsoft's Aquantive--it uses, or what broadband providers it counts as customers. So did Phorm and Front Porch (which said it could not arrange an interview). When asked why it won't disclose that information, NebuAd told us in e-mail: 'We would like to respect the trust and relationship that already exists between an ISP and their end customer. We want to stress that we do not publicly discuss our ISP partner relationships because of the direct relationship that already exists between an ISP and their customers. Our belief is that our ISP partners have a direct, trusted relationship with their customers; and communication, public or otherwise, should be directly from our ISP partner to their end customer.'").

[14] *See e.g.* AT&T Privacy Policy for AT&T Yahoo! *infra* note 16, http://helpme.att.net/article.php?item=8620 (last visited September 30, 2008).

[15] *See* Embarq response to letter from congressmen Joe Barton, Edward Markey and John Dingell, BroadcastingCable.com, http://www.broadcastingcable.com/contents/pdf/EmbarqResponse.pdf (last visited September 30, 2008).

[16] *See e.g.* AT&T Privacy Policy for AT&T Yahoo! and Video Services, For All Applications, All Operating Systems, and All Domains, http://helpme.att.net/article.php?item=8620 (last visited September 30, 2008) ("AT&T uses Usage Information to personalize your Services, to recommend content, and to select advertisements or other

sometimes unclear, but a close reading reveals that they are in fact placing users on notice that their communications can and often will be inspected for any reason.[17] The user functionally waives any and all privacy expectations against the IAP. AT&T's subscriber agreement goes so far as to claim ownership over user communications, which are deemed to be the business records of AT&T.[18] The IAPs' subscriber contracts require users to waive privacy by consenting to the monitoring of their online activities. ***This is a mandatory condition of receiving service.***

b. The Destruction of All Online Privacy Rights

The IAPs typically make promises and commitments regarding the use they will make of the private information they capture. While that is laudable, it does not serve to preserve or "unwaive" privacy.[19] Under the law, once confidentiality has been waived as to one party or destroyed through inspection, it is waived as to all.[20] While IAP privacy policies and the behavioral advertising vendors may make certain promises to protect or respect the privacy of the users, these reassurances are wholly ineffective because confidentiality has already been destroyed by user consent to inspection. Under what has been termed the Third Party Doctrine, one cannot maintain a reasonable expectation of privacy in any information that is knowingly

---

promotions for you based upon your interests. … We may disclose Aggregated Information to third parties including advertisers, content providers, market research companies and other organizations.").

[17] A recent report analyzed the readability of various IAP privacy policies and determined that almost all required at least a college level education to understand the policies. A number were scored at post-graduate levels of readability. *See* Erik Sherman, Privacy Policies are Great – PhDs, BNet.com, http://industry.bnet.com/technology/1000391/privacy-policies-are-great-for-phds/ (last visited September 30, 2008).

[18] *See* AT&T Privacy Policy for AT&T Yahoo! *supra* note 16, http://helpme.att.net/article.php?item=8620 (last visited September 30, 2008) ("While your Account Information may be personal to you, these records constitute business records that are owned by AT&T. As such, AT&T may disclose such records to protect its legitimate business interests, safeguard others, or respond to legal process.").

[19] *See* Jennifer A. Hardgrove, *Scope of Waiver of Attorney-Client Privilege: Articulating a Standard That Will Afford Guidance to Courts*, 1998 U. Ill. L. Rev. 643, 653 (1998) ("Voluntary disclosure of a privileged communication constitutes a waiver in nearly all situations, even where the disclosure was nontruthful or misstated, where the disclosed information could have been obtained elsewhere, and where the third party receiving the disclosed information agreed not to further disclose it.") (Emphasis added).

[20] Because confidentiality requires that a communication stay entirely out of the purview of *any* unintended parties, once the confidence has been vitiated through disclosure, it cannot be reestablished. The presence of the unintended party will always frustrate confidentiality as to all relationships. In this respect, confidentiality is much like Humpty Dumpty, once it has been broken, it cannot be put back together again.

disclosed to a third party. Because users are required to consent to DPI and the monitoring of their online communications, they have knowingly disclosed this private information to a third party. The result is that any expectation of privacy the user may have is unreasonable as a matter of law.

This combination of inspection and waiver now threatens to profoundly change the way online privacy rights are determined. Heretofore the courts have assumed that contents are not generally inspected and Internet communications have traditionally been held to the same privacy and privilege standard as private telephone and mail communications. The information can be obtainable only by warrant[21] or a subpoena directed at one of the communicants. With the introduction of DPI to perform behavioral advertising, user communications are no longer carried without inspection. Confidentiality is destroyed through third party access.[22] Because confidentiality is an essential element of common law and statutory privileges, an inspected Internet is incapable of carrying privileged communications.[23] Those who wish to maintain privileged relationships can no longer communicate in confidence over an Internet that is monitored by their IAPs. These communications will be treated as all other non-confidential

---

[21] See *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) ("In a sense, e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission. The sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police."); *United States v. Charbonneau*, 979 F.Supp. 1177, 1184 (D. Ohio 1997) ("E-Mail is almost equivalent to sending a letter via the mails.").

[22] *See United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) ("The policy clearly stated that FBIS would "audit, inspect, and/or monitor" employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate." J.A. 127. This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private.").

[23] The leading privilege test was established in *United States v. United Shoe Machinery Corp.* 89 F. Supp. 357, 358-59 (D. Mass. 1950). The *United Shoe* test provides that a privilege (in this instance between an attorney and a client) applies if:

> (1) the asserted holder of the privilege is or sought to become a client; (2) the person to whom the communication was made (a) is the member of the bar of court, on his subordinate and (b) in connection with this communication is acting as a lawyer; (3) the communication relates to a fact of which the attorney was informed (a) by his client (b) without the presence of strangers (c) for the purpose of securing primarily either (i) an opinion of law or (ii) legal services or (iii) assistance in some legal preceding, and not (d) for the propose of committing a crime or tort; and (4) the privilege has been (a) claimed and (b) not waived by the client. (emphasis added).

communications and will be freely accessible to outside parties with a subpoena to the IAP based on a mere showing that production *may* lead to the discovery of relevant evidence.[24] The communication will be disclosed before the privilege holder ever gets notice or a chance to assert the privilege. Important confidential and privileged communications would be available to anyone under the very lax standard of mere relevance. Any and all privileges will have been waived by simply accessing the inspected network.

It is not just the confidentiality of communications between private individuals that are threatened by DPI and network-based behavioral advertising. The Internet has been incorporated into virtually every American industry as a means of efficiently carrying out transactions and communications. Businesses use the Internet to communicate externally with consumers and other companies, as well as internally amongst employees and facilities. A huge portion of these online communications contain proprietary information and trade secrets that are intended to remain confidential, often being subject to non-disclosure agreements. But with an IAP inspected Internet, even business trade secrets and other confidential business information loses all protection. Ecommerce may grind to a halt because sensitive information will have to be communicated "the old fashioned way." That could very well put the nail in our country's economic coffin.

VIII. Declaration of Public Policy Against Abusive Subscriber Contracts

Under the current self-regulatory framework, those that would violate the privacy rights of America's Internet users are subject to little accountability. IAPs and advertising systems

[24] *See* Fed. Rules Civ. Proc. R. 26(b)(1) ("Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.") (Emphasis added).

vendors are free to wiretap their users communications and peer into their most private online activities with no fear of repercussion. Users cannot adequately protect their privacy rights and guard themselves against potentially abusive network practices and subscriber contracts.

While DPI and network-based behavioral advertising need not be prohibited, they should only be permitted once users have expressly and knowingly opted-in to the practices. Requiring this consent as a mandatory condition of service is not voluntary and is fundamentally opposed to the FTC's proposed principles of affirmative express consent and consumer control. Ensuring voluntary and informed user consent to potentially harmful subscriber contracts and network practices falls in line with the intent of the proposed principles and the expectations of Internet users.

To ensure that the new privacy principles, as well as the Fair Information Practice Principles, are uniformly observed throughout the industry, the FTC has a responsibility to provide users with a means to protect themselves against mistreatment. While intrusive regulation would likely stifle innovation and lead to burdensome administrative oversight, there is a solution that can protect user privacy and is consistent with the notion of deregulation. Data Foundry requests that the FTC formally recognize a public policy against abusive Internet access contracts that require consumers to waive their privacy rights as a condition of service and provide inadequate disclosure of network practices and their subsequent effects upon user privacy.

Public policies are privately enforceable in state and federal courts of law without any need for further administrative or regulatory action. Individual citizens that are injured by these exploitative subscriber agreements and behavioral advertising practices would have the right to bring claims against their IAPs under traditional principles of contract law that prohibit

violations of established public policies. This stated policy would merely hold IAPs and advertising vendors accountable to their customers through judicial remedies, in the same manner as all other deregulated contract relationships. The policy would protect the privacy of online communications from an especially insidious form of invasion and provide a much-needed safeguard against abuse, without the need for burdensome regulation.

IX. Conclusion

Data Foundry is grateful to the FTC for the opportunity to address these important and involved matters. The privacy issues inherent in behavioral advertising present difficult challenges to ensuring an innovative and safe Internet. We hope that the FTC will recognize the particularly invasive nature of DPI-facilitated behavioral advertising and the harmful effects of the subscriber agreements that require users consent to inspection and waive their privacy rights as conditions of service. By declaring a public policy against such contracts (rather than trying to devise *ex post* and *ex ante* rules and procedures and an administrative enforcement process), the FTC would be treating Internet access like all other "unregulated" activities. It would be a simple matter of contract and consumer law, handled at the state level. But it would provide Internet users with the necessary means to protect their privacy. At the same time, it would ensure that "the Internet" is not burdened by intrusive administrative regulation.

Respectfully Submitted,

/s/
Ron Yokubaitis
Chairman and CEO, Data Foundry, Inc.